UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | : | |
| *– against –* | : | |
| | : | 12 Cr. 045 (RJS) |
| JERMAINE DORE (2), | : | Electronically Filed |
| Defendant. | : | |

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT JERMAINE DORE'S PRETRIAL MOTION TO SUPPRESS CELL SITE EVIDENCE

Alice L. Fontier, Esq.
DRATEL & MYSLIWIEC, P.C.
2 Wall Street, 3rd Floor
New York, New York 10005
Tel: (212) 732-0707
Afontier@dratelmys.com

*Attorney for Defendant*
*Jermaine Dore*

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | : | |
| – *against* – | : | |
| | : | 12 Cr. 045 (RJS) |
| JERMAINE DORE (2), | : | Electronically Filed |
| Defendant. | : | |

## INTRODUCTION

This memorandum of law is submitted in support of defendant Jermaine Dore's pretrial motion pursuant to Rule 12(b), Fed.R.Crim.P., to suppress historical cell site evidence that was obtained pursuant to a warrantless search.

The historical cell site evidence should be suppressed because it was obtained by a warrantless search that was not supported by probable cause. The Stored Communications Act, which permits the Court to Order the release of historical cell site evidence on less than probable cause is unconstitutional as applied to Mr. Dore. In addition, even if the Court finds that the Stored Communications Act is constitutional as applied, the historical cell site evidence at issue here must still be suppressed because the application did not set forth "specific and articulable facts" sufficient to demonstrate that the scope of material sought was relevant and material to an ongoing investigation of Mr. Dore. 18 U.S.C. § 2703(d).

Accordingly, Mr. Dore moves for suppression of the historical cell site evidence.

## STATEMENT OF FACTS

Mr. Dore, along with four co-defendants, is charged in an Indictment with conspiracy to commit robbery, in violation of 18 U.S.C. § 1951(b)(1), and using a firearm in connection with a crime of violence, in violation of 18 U.S.C. § 924(j), among other substantive offenses.[1]

The evidence against Mr. Dore relies heavily on information gleaned from the historical cell site evidence obtained from telephone companies without a warrant. The government sought and received the historical cell site evidence pursuant to several Orders. Copies of which are attached to the Fontier Dec., as Exhibit 1. The Orders, issued pursuant to 18 U.S.C. § 2703(d), directed the telephone companies to release historical cell site evidence on several cell phones from November 1, 2010 through January 12, 2012, a period of one year, two months, and twelve days (438 days).

The application for the release of the historical cell site evidence contained information pertaining to a robbery that occurred on October 11, 2011 in New Rochelle, New York. *See* Application for Cell Site Evidence ("Application"), attached to the Fontier Dec. as Exhibit 2. The facts that pertain to Mr. Dore are limited to the following:

> [a]n analysis of call records reveals that Todd's cellular telephone was in contact with Target Cellphone-5, believed to be used by Jermaine Dore, shortly before this robbery took place, and in turn, Target Cellphone-5, believed to be used by Dore, was in contact with Target Cellphone-1, believed to be used by Fahd Hussein, shortly after this robbery took place.

Application at 4. The application does not set forth any other facts that establish that the historical cell site evidence was relevant or material to the investigation.

---

[1] Counsel for co-defendants indicated that they would join this Motion to the extent that it inures to the benefit of their clients.

## ARGUMENT

### The Court Should Suppress the Historical Cell Site Evidence Because It Was Obtained In Violation of the Forth Amendment

The Fourth Amendment protects against "unreasonable searches and seizures" and guarantees that the right "shall not be violated, and no Warrants shall issue, but upon probable cause[.]" U.S. Consitution, Amend. IV. Historical cell site evidence effectively produces a map of the telephone users every movement. The use of electronic surveillance to track a person's every movement over a prolonged period of time raises Fourth Amendment concerns, that must be protected by the warrant requirement.

#### 1. Cumulative Historical Cell Site Evidence is Protected By the Fourth Amendment

The Supreme Court recently held that the warrantless use of GPS tracking violates the Fourth Amendment. *United States v. Jones* __ U.S. __, 132 S.Ct. 945 (2012). The use of historical cell site evidence to track a person's movements raises the same privacy concerns and is similarly protected by the Fourth Amendment.

In *Jones* the majority of the Court, in holding that the warrantless use of a GPS tracker violated the Fourth Amendment, focused on the trespassory nature of physically attaching the GPS tracker to the vehicle. *Jones*, 132 S.Ct. at 949. However, Justice Sotomayer in a concurring opinion stressed that,

> the Fourth Amendment is not concerned only with trespassory intrusions on property. See, *e.g., Kyllo v. United States,* 533 U.S. 27, 31–33, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). Rather, even in the absence of a trespass, "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy

> that society recognizes as reasonable." *Id.,* at 33, 121 S.Ct. 2038; see also *Smith v. Maryland,* 442 U.S. 735, 740–741, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); *Katz v. United States,* 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring).

*Jones*, 132 S. Ct. 954-55 (Sotomayor, J., concurring). Justice Sotomayor continued:

> physical intrusion is now unnecessary to many forms of surveillance. *Post,* at 961 – 963. *With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones.* See *United States v. Pineda–Moreno,* 617 F.3d 1120, 1125 (C.A.9 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc). In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Ante,* at 953. As Justice Alito incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. *Post,* at 962 – 963. *Under that rubric, I agree with Justice Alito that, at the very least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Post,* at 964.

*Id*. at 955, emphasis added.

Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan issued a separate concurring opinion in *Jones*. Justice Alito argued against the majority's focus on the physical trespass in part because it "will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked." *Jones*, 132 S. Ct. at 962 (Alito, J., concurring). Justice Alito argued that focusing on the trespass did little to protect the Fourth Amendment concerns of most people, in light of new technologies. Justice Alito noted that, "[p]erhaps most significant, cell phones and

other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States." *Id*., at 963.

In light of these concerns, Justice Alito concluded:

> [t]he best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.
>
> Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See *Knotts,* 460 U.S., at 281–282, 103 S.Ct. 1081. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, *society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.* In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark.

*Id*., at 964, emphasis added.

Thus, as a District Court in Maryland noted, "it appears as though a five justice majority is willing to accept the principle that government surveillance over time *can* implicate an individual's reasonable expectation of privacy." *United States v. Graham*, 846 F. Supp. 2d 384, 394 (D. Md. 2012). Recently, a District Court in Pennsylvania concluded that "taken together, the installation of the GPS tracker and subsequent monitoring constitute a significant intrusion on Fourth Amendment privacy rights." *United States v. Ortiz*, CRIM.A.__ F.Supp.2d. __, 2012 WL 2951391 (E.D. Pa. July 20, 2012).

The same privacy concerns at issue in the recent GPS cases are at issue here. The historical cell site data tracks every movement of a person over a prolonged period of time. As Justice Sotomayor noted in *Jones*,

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.

*Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

Accordingly, despite some case law to the contrary, *see e.g. Graham*, 846 F. Supp. 2d 384, this Court should adopt the findings set forth by Judge Garaufis in the Eastern District of New York, in *In the Matter of the Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F.Supp.2d 113 (EDNY 2011) (hereinafter "Garaufis Opinion").

In that case, decided prior to *Jones*, Judge Garaufis denied the application for release of historical cell site evidence because he found that despite the Stored Communications Act ("SCA"), the Fourth Amendment requires a showing of probable cause and the issuance of a warrant before long-term historical cell site data could be released. *Id*, at 127. Relying on the D.C. Circuit's decision in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010) – the underlying case in *Jones* which was affirmed by the Supreme Court – Judge Garaufis concluded that a request for long-term historical cell site data constituted a search which implicates the Fourth Amendment.

Judge Garaufis explained the holding of *Maynard* as follows:

> [t]he *Maynard* court noted two important distinctions between the short-term surveillance in *Knotts* and the prolonged surveillance at issue in *Maynard.* First, the court concluded that while the individual in *Katz* did not have a reasonable expectation of privacy over his location while traveling from one place to another, the individual in *Maynard* had a reasonable expectation of privacy over the *totality* of his movements over the course of a month. The court reasoned that the totality of one's movements over an extended time period is not actually exposed to the public "because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil." *Maynard,* 615 F.3d at 560. Second, the court concluded that people have an objectively reasonable expectation of privacy in the totality of their movements over an extended period because an individual's privacy interests in the totality of his movements far exceeds any privacy interest in a single public trip from one place to another.

*Garaufis Opinion*, 809 F. Supp. 2d at 118.

Following this reasoning, Judge Garaufis concluded that the cell site data at issue – a request for 113 days of records – sought information that is protected by the Fourth Amendment. *Id*. at 119. Judge Garaufis held, "[t]he cell-site-location records sought here captures enough of the user's location information for a long enough time period—significantly longer than the four weeks in *Maynard*—to depict a sufficiently detailed and intimate picture of his movements to trigger the same constitutional concerns as the GPS data in *Maynard.*" *Id.* Here, the government's request was for 438 days of records – nearly four times that at issue in the Garaufis matter. More significantly the information obtained in this case was for a period that is almost fifteen times longer, than the four week period at issue in *Jones*, which Justice Sotomayor declared was certainly past the point where a search had occurred. *Jones*, 132 S. Ct. at 956. (Sotomayor, J., concurring).

Accordingly, the cell site evidence obtained by the government about Mr. Dore – 438 days of information – was protected by the Fourth Amendment, and should not have been released without a warrant based on probable cause.

The cases that hold to the contrary, hold that a person does not have a reasonable expectation of privacy in the cell site data because that information is voluntarily provided to a third-party. *See e.g. Graham*, 846 F. Supp. 2d 384, 389 ("These courts [that have held that the Fourth Amendment does not apply to historical cell site data] have primarily relied on a line of Supreme Court cases construing the scope of Fourth Amendment rights relating to business records held by third parties. More specifically, these courts have concluded that because people voluntarily convey their cell site location data to their cellular providers, they relinquish any expectation of privacy over those records."). However, as Judge Garaufis held,

> [t]he cell-site-location records at issue here currently enable the tracking of the vast majority of Americans. Thus, the collection of cell-site-location records effectively enables "mass" or "wholesale" electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip. This further supports the court's conclusion that cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records and that the Government's obtaining these records constitutes a Fourth Amendment search.

*Garaufis Opinion*, 809 F. Supp. 2d at 119-20.

Indeed, as Justice Sotomayor noted:

> [m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith* [*v. Maryland*], 442 U.S. [735], at 742 [(1979)]; *United States v. Miller,* 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone

> numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post,* at 962, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

*Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

Given the Supreme Court's view, this Court should follow the holding in the Garaufis Opinion. There, Judge Garaufis held that "an exception to the third-party-disclosure doctrine should be applied to the *cumulative* cell-site-location records." *Garaufis Opinion*, 809 F. Supp. 2d at 122. Judge Garaufis reasoned that "[t]he Supreme Court and lower appellate courts have recognized an exception to the third-party-disclosure doctrine in a subset of cases in which the content of the information communicated would be revealed through the Government's surveillance ('content exception')." *Id.* Judge Garaufis continued, "the content exception preserves the reasonable expectation of privacy, and thus Fourth Amendment protection, for some information to which strict application of the *Katz* test and the third-party-disclosure doctrine would not permit. Carving this exception out of the *Katz* test is consistent with Supreme Court precedent, which has long recognized that the *Katz* test may fail to provide sufficient Fourth Amendment protections in some cases." *Id.* at 123.

Applying the "content exception" to cell-site evidence, the court concluded:

> that established normative privacy considerations support the conclusion that the reasonable expectation of privacy is preserved here, despite the fact that cell-site-location records is disclosed to cell-phone service providers. Applying the third-party-disclosure doctrine to cumulative cell-site-location records would permit governmental intrusion into information which is objectively recognized as highly private. *See Maynard*, 615 F.3d at 555. Following the decision in *Maynard*, this court concludes that cumulative cell-site-location records implicate sufficiently serious protected privacy concerns that an exception to the third-party-disclosure doctrine should apply to them, as it does to content, to prohibit undue governmental intrusion. Consequently, the court concludes that an exception to the third-party-disclosure doctrine applies here because cell-phone users have a reasonable expectation of privacy in cumulative cell-site-location records, despite the fact that those records are collected and stored by a third party.

*Id.* at 126.

This Court should follow the reasoning in the Garaufis Opinion, and hold that the Fourth Amendment applies to the search of Mr. Dore's historical cell site data, and that the third-party disclosure doctrine does not eliminate the reasonable expectation of privacy. Mr. Dore's every movement for a period of one year, two months, and twelve days has been provided to the government. This level of intrusion into his private life is protected by the Fourth Amendment. As the government did not have a warrant, or probable cause, to seek this information, it should now be suppressed.

**2. The Stored Communications Act is Unconstitutional as Applied**

The Stored Communications Act authorizes the release of historical cell site data to a governmental entity "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic

communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C.A. § 2703(d). "[T]he 'specific and articulable facts' standard contained in the Stored Communications Act is a lesser one than probable cause. *See In re Application of the United States,* 620 F.3d at 313–15 (3d Cir.2010)." *Graham*, 846 F. Supp. at 396.

Mr. Dore contends that the Application obtained pursuant to the SCA is invalid because the SCA is unconstitutional as applied to him in this case. As a court in the Eastern District has described,

> [i]n an as-applied challenge, the question is whether the statute would be unconstitutional if applied literally to the facts of the case. *Cf. Field Day LLC v. County of Suffolk,* 463 F.3d 167, 174 (2d Cir.2006). Factual context and defendant's circumstances are critical. *See, e.g., Arzberger,* 592 F.Supp.2d at 599. A sequential analysis, putting off facial challenges, permits the courts to protect the constitutional rights of individual defendants in particular situations, while avoiding the unnecessary striking down of a congressional enactment. *See Washington State Grange v. Washington State Republican Party,* 552 U.S. 442, 450, 128 S.Ct. 1184, 170 L.Ed.2d 151 (2008) (noting that facial invalidation contravenes the "fundamental principle ... that courts ... should [not] formulate a rule of constitutional law broader than is required by the precise facts to which it is applied").

*United States v. Polouizzi*, 697 F. Supp. 2d 381, 387 (E.D.N.Y. 2010). Mr. Dore does not challenge the facial constitutionality of the SCA, he only argues that it is unconstitutional as applied in this case.

For the reasons set forth **ante** in Point 1, the scope of the request in this case for 438 days of historical cell site data is so broad, and gathers so much personal evidence about Mr. Dore, that the cumulative effect constitutes a search and is subject to Fourth Amendment protections.

The government was required to make a showing of probable cause and obtain a warrant prior to receiving 438 days of records. Because the SCA only requires a showing of "specific and articulable facts" – a standard below probable cause – the SCA is unconstitutional as applied to Mr. Dore.

Accordingly, this Court should suppress the historical cell site evidence.

**3. The Application for Historical Cell Site Evidence Was Not Sufficient to Meet the "Specific and Articulable" Facts Test**

Even if this Court finds that the Fourth Amendment does not apply to historical cell-site evidence, the cell site data pertaining to Mr. Dore must still be suppressed. The Application for the Order fails to meet even the reduced "specific and articulable" facts requirement set forth in the SCA.

As stated **ante**, the *only* facts that pertain to Mr. Dore in the Application are limited to the following:

> [a]n analysis of call records reveals that Todd's cellular telephone was in contact with Target Cellphone-5, believed to be used by Jermaine Dore, shortly before this robbery took place, and in turn, Target Cellphone-5, believed to be used by Dore, was in contact with Target Cellphone-1, believed to be used by Fahd Hussein, shortly after this robbery took place.

Application at 4.

Two telephone calls at or near the time of a robbery do not amount to sufficient and articulable facts sufficient to justify the release of one year, two months, and twelve days worth of records. Indeed, there is no information in the Application about the numbers of calls between Mr. Dore and any of his other co-defendants at times other than at or near the time of a single alleged robbery. Yet the phone records reveal that there are multiple calls between Mr. Dore and

his co-defendants at all different times, which do not correspond to any alleged criminal conduct. Certainly, two phone calls taken out of context does not provide any basis for concluding that the calls were part of a pattern of criminality as the Application suggests.

In *United States v. Leon*, 468 U.S. 897, the Supreme Court established the good faith exception to the warrant requirement. There, the Court held that, even if a warrant was later found to be improper, so long as the officers relying on the warrant conducted the search in an objectively reasonable manner then suppression is not warranted. *Id.* at 922. The Second Circuit has explained that if the warrant is improper and "no reasonably well-trained police officer could believe otherwise[,]" then the good-faith exception does not apply. *United States v. George,* 975 F.2d 72, 77 (2d Cir. 1992). Here, the Application is nearly devoid of facts and reliance on it was patently improper, thus the good-faith exception does not apply.

Accordingly, because the Application is insufficient to meet the "specific and articulable facts" requirement of the SCA, this Court should suppress the historical cell site data.

**4. The Exclusionary Rule is the Appropriate Remedy**

In determining whether to suppress evidence obtained in violation of the Fourth Amendment, "the Court must apply the general standard for application of the exclusionary rule: whether 'the benefits of deterrence ... outweigh the costs' of the application of the exclusionary rule." *Ortiz*, at *24, internal citations omitted.

In *Ortiz*, the Court held that the exclusionary rule was the appropriate remedy for GPS tracking data obtained without a warrant. *Id*. There the government argued that the officers had acted reasonably in good-faith reliance on what they believed to be DEA policy. *Id.* Rejecting this argument the Court held "[t]he solution is simple: the import of [*Davis v. United States*, __

U.S. __, 131 S.Ct. 2419 (2011)] is that officers acting without clearly applicable binding appellate guidance should err on the side of caution and obtain a warrant." *Id.*

Here, the government could have sought a warrant – based on probable cause – as was required by the Fourth Amendment, but chose instead to rely on a lesser standard. As in *Ortiz*, the appropriate remedy for this Constitutional violation is suppression of the cell site data.

**CONCLUSION**

For the foregoing reasons, it is respectfully submitted that the Court should suppress the cell site data obtained as the fruit of an unlawful search and seizure.

Dated: September 28, 2012
New York, New York

Respectfully submitted,

/S/ Alice L. Fontier
Alice L. Fontier
DRATEL & MYSLIWIEC, P.C.
2 Wall Street, 3rd Floor
New York, New York 10005
(212) 732-0707
Afontier@dratelmys.com

*Attorney for Defendant Jermaine Dore*